REMARKS

The Examiner rejected Claims 1, 3-7, 13, 15-19, 25, and 27-31 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,278,901 to Shieh et al. (Shieh), in view of U.S. Patent No. 5,440,723 to Arnold et al. (Arnold), and further in view of U.S. Patent No. 5,832,208 to Chen et al. (Chen). Applicant respectfully disagrees with such rejection.

Specifically, in the Examiner's latest response to applicant's previous arguments, the Examiner relies on the following teaching of Shieh (in combination with Chen) to make a prior art showing of applicant's claimed "wherein one of said measurement parameters is how many e-mail messages are sent having an identical message title" (see all pending independent claims).

> "The indirect-write pattern of virus propagation, namely Iw(virus, o_i), may appear individually or simultaneously and can be detected by the model of the present invention using the following conditions: (1) |v.. set(out, Iw/Iw*, virus)|>threshold and a large portion of elements are executable files; (2) |C.. set(out, Iw/Iw*, virus)|>threshold; (3) |v.. set(in, cb/cb*/Icb/Icb*, virus)|>threshold; (4) |C.. set(in, cb/cb*/Icb/Icb*, virus)|>threshold; (5) v.. set(out, Id/Id*, virus)|>threshold; (6) |C.. set(out, Id/Id*, virus)|>threshold. The used here are parameters defining limits to determine abnormal process behavior. If the occurrences of a pattern exceeds the threshold, an abnormality occurs." (col. 17, lines 17-30)

With respect to Chen, the Examiner relies on the following excerpt (in combination with the foregoing Shieh excerpt) to make a prior art showing of the foregoing claim limitations:

> "Of particular concern in relation to the transmission of computer viruses is electronic mail (e-mail). There is a growing use of e-mail to communicate within an organization (e.g., using a local area network) and to communicate externally (e.g., over the Internet with computer users located at remote locations). E-mail messages may include attached files containing, for example executable programs, formatted documents, sound, video, etc. It will be appreciated that an attachment to an e-mail message may contain a file infected with a computer virus. Thus, for example, an e-mail message received over the Internet may contain as an attachment a Microsoft Word document infected with a Word Macro virus; an e-mail message broadcast on the local area network by a project manager to her many team members may contain an attachment also infected with a virus." (col. 3, lines 17-32)

The Examiner continues by arguing that "because Chen teaches the danger of email attachments in association with viruses, ... it would have been obvious to one having ordinary skill in the art to monitor all characteristics of a broadcast email. Specifically these threshold parameters would include email subject line, since a broadcast email would have the same subject line."

Applicant respectfully disagrees with this assertion. First, Chen's focus on the danger of attachments *teaches away* from any sort of "how many e-mail messages are sent having an identical message title," as claimed by applicant. Specifically, the review of attachments would, in no way, involve analysis of e-mail message titles, let alone "how many e-mail messages are sent having an identical message title." By specifically addressing only attachments and not e-mail messages themselves (i.e. e-mail message titles, etc.), Chen *teaches away* from applicant's claimed invention. Only applicant teaches and claims the specific analysis of the number of e-mail messages that are sent having an identical message title for the specific purpose of detecting virus-related behavior, independent of attachments, etc.

The Examiner argues that the proposed combination, when broadly interpreted, meets applicant's claim limitations, and asserts that no Official Notice is invoked. In reviewing the Examiner's proposed combination, however, there is not even a suggestion of monitoring e-mail message titles, let alone "how many e-mail messages are sent having an identical message title." From the Examiner's argument that the "threshold parameters would include email subject line, since a broadcast email would have the same subject line," applicant is left to assume that the Examiner is relying on an *inherency* argument (since the Examiner is relying on subject matter not in the explicit teachings of the combined references).

In view of the foregoing arguments made hereinabove, any such *inherency* argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

Applicant further notes that the Examiner has not even fully considered and/or responded to applicant's previous arguments. Specifically, the Examiner has relied on the following excerpt from Shieh to meet applicant's claimed measuring "one or more measurement parameters indicative of

non virus specific activity of said computer apparatus over a respective measurement period" and comparing "said one or more measurement parameters with respective predetermined threshold levels."

> "The indirect-write pattern of virus propagation, namely Iw(virus, o_i), may appear individually or simultaneously and can be detected by the model of the present invention using the following conditions: (1) |v-- set(out, Iw/Iw*, virus)|>threshold and a large portion of elements are executable files; (2) |C-- set(out, Iw/Iw*, virus)|>threshold; (3) |v-- set(in, cb/cb*/Icb/Icb*, virus)|>threshold; (4) |C-- set(in, cb/cb*/Icb/Icb*, virus)|>threshold; (5) v-- set(out, Id/Id*, virus)|>threshold; (6) |C-- set(out, Id/Id*, virus)|>threshold. The used here are parameters defining limits to determine abnormal process behavior. If the occurrences of a pattern exceeds the threshold, an abnormality occurs." (col. 17, lines 17-30)

Such excerpt along with the remaining Shieh reference, however, fails to disclose, teach or even suggest applicant's claimed "one or more measurement parameters indicative of non virus specific activity of said computer apparatus over a respective measurement period" (emphasis added).

Specifically, each of the conditions mentioned in the above excerpt are a function of a "virus," and thus do not meet applicant's claimed specific measurement parameters that are indicative of non virus specific activity. Only applicant teaches and claims such a threshold-based virus detection method that is based on non virus specific activity, as specifically claimed.

Further, the conditions outlined in the Shieh reference make absolutely no mention of any time dependence. Thus, Shieh fails to meet applicant's claimed measurement of the related parameters over a respective measurement period. This feature is clearly absent in Shieh, as is evidenced by the foregoing excerpt.

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations

It appears that the Examiner has made similar deficient arguments with respect to applicant's dependent claims. Just by way of example, applicant can not find any explicit suggestion of the following claimed subject matter, in the Examiner's proposed combination:

"wherein one of said measurement parameters is how many e-mail messages are sent having an identical file attachment" (see Claim 3 et al.);

"wherein one of said measurement parameters is how many e-mail messages are sent having a file attachment of a given file type" (see Claim 4 et al.);

"wherein one of said measurement parameters is e-mail throughput within said computer system" (see Claim 6 et al.); and

"wherein each e-mail processed has an associated size value and e-mail throughput is measured in a form dependent upon a number of e-mails multiplied by a total of size values for said e-mails" (see Claim 7 et al.).

Since the Examiner is relying on teachings that are not explicitly set forth in the proposed combination, applicant assumes that the Examiner is again relying on an *inherency* argument. The foregoing features, however, provide particular advantage over the Examiner's proposed combination, by reviewing specific types of activity (that are not even suggested by the Examiner's combination) which may possibly be initiated by a virus.

Again, in view of the foregoing arguments made hereinabove, any such *inherency* argument has been adequately rebutted, and a notice of allowance or a specific prior art showing of such claim features, in combination with the remaining claim elements is respectfully requested. (See MPEP 2112)

A notice of allowance is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P154).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100